UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/880,470	06/13/2001	Radia J. Perlman	P5761	5216

25181 7590 11/30/2004

FOLEY HOAG, LLP
PATENT GROUP, WORLD TRADE CENTER WEST
155 SEAPORT BLVD
BOSTON, MA 02110

EXAMINER	
POLTORAK, PIOTR	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 11/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

8

Office Action Summary	**Application No.** 09/880,470	**Applicant(s)** PERLMAN, RADIA J.	
	Examiner Peter Poltorak	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *30* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-36 have been examined.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1, 3, 16, 18, 22, 23, 25, 29, 34 and 35 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. Claim 1 recites "said second node" in line 16-17 pg. 19. There is insufficient antecedent basis for this limitation in the claim.

   Also, it is not clear whether "a second node" cited in line 19 is a different node or whether it is the same node and simply the order of lines 16-17 and 18-19 have been mistakenly changed (if so it is not clear whether the order of steps is important and which one is correct).

4. Claim 3 as stated removes a limitation from claim 1 on which claim 3 depends. As a result, claim 3 has a broader scope than claim1.

5. Claims 29 and 34 present similar problems and are similarly rejected.

6. Claim 16 places a limitation of deleting said first secret key at said second node but in claim 15 on which claim 16 depends it is suggested that decryption of the first secret key and decrypting the encrypted information value using the first secret key is done at the third node. As result, it appears as though a step is missing.

7. Claim 18 teaches a step of "verifying .. to ascertain whether the second node is an authorized decryption agent" and further cites the limitation "in response to verification that the second node is an authorized decryption agent". It is not clear whether the limitation requires a positive result of the verification before the first node is to communicate the value to the second node or whether the communication of the value occurs as long as there is any verification.
8. Claims 18, 22, 23 and 35 the use term "decryption agent" which is not understood. Similarly the "proof" cited in claims 18, 22, 23, 30 and 35 is not understood.
9. In claim 22, lines 11 and 13, "said first public key" lacks antecedent basis.
10. In claim 25, lines 8-9, "said third encryption and decryption keys" lacks antecedent basis.
11. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

12. Claims 1-10, 15, 17, 27-29 and 32-34 are rejected under 35 U.S.C. 102(e) as being anticipated by *Hanna (U.S. Pub. No.2002/0136410)*. The applied

reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

13. *Hanna* teaches an invention relating to methods and apparatus for assuring data security and more specifically, to techniques for extinguishing ephemeral keys to prevent encrypted information from being decrypted using an ephemeral key following a predetermined expiration time for the respective ephemeral key *[0003]* and further discloses party A including the doubly encrypted symmetric key in the message, as well as indications of the ephemerizer and ephemeral encryption key, and passing the complete message to party B. Upon receipt of the message from party A, party B sends the doubly encrypted symmetric key to the ephemerizer indicated within the message. The ephemerizer applies the appropriate ephemeral decryption key to the doubly encrypted symmetric key, for example using a private key from an ephemeral key pair also including the public key used as the ephemeral encryption key for the message. The result of this decryption is a copy of the symmetric key still encrypted by the encryption key of party B. The ephemerizer passes this still encrypted symmetric key back to Party B, which then uses its own decryption key to complete decrypting the symmetric key.

Party B uses the completely decrypted symmetric key to decrypt the body of the message *[0039] and [0040]*.

The teaching reads on "securely communicating said doubly wrapped value to said second node, obtaining a second decryption key having a predetermined expiration time at a second node, decrypting said doubly wrapped value using said second decryption key to produce said singly wrapped value if said second decryption key has not expired and securely communicating said singly wrapped value to a third node."

Furthermore *Hanna* teaches: multiple ephemerizers that may be used to successively encrypt the message symmetric key and the message key portion of the ephemeral message format including a symmetric key which was used to encrypt the message body, and which has been successively encrypted with each of the ephemeral encryption keys 1 through N of the ephemerizers 1 through N. Accordingly, in order to decrypt the message body, the receiver must use each of the ephemerizers 1 through N to successively decrypt the symmetric key in the message, so that the message body may be decrypted using the decrypted symmetric key *[0042] which reads on* decrypting the triply wrapped value using a third decryption key associated with the third encryption key to obtain the doubly wrapped value and securely communicating said doubly wrapped value to the second node.

This also reads on the limitation of claim 2: generating in a fourth node said triply wrapped value and communicating the triply wrapped value for receipt by the first node.

As per claim 3 the first node and the third node are the same node *[0039-0040]*.

The limitations of claim 8 are inherent. The singly wrapped value is a part of doubly and triply wrapped values.

As per claims 9-10 *Hanna* teaches the parties 1 through party M, being communicative with the ephemerizers, via a communications or messaging infrastructure such as a computer network or the Internet *[0034]* and the ephemeral message format including an ephemerizer identifier identifying one of the ephemerizers, such as a Uniform Resource Locator (URL), Internet Protocol (IP) address and port number combination, or other type of name or address information. The message format further includes an ephemeral encryption key identifier, such as an index, remote reference, or pointer, for example indicating an ephemeral key pair within an ephemeral key pair list published by the ephemerizer identified by the ephemerizer identifier. Alternatively, the ephemeral encryption key identifier may indicate an ephemeral symmetric key known by that ephemerizer. A message key portion includes a symmetric key encrypted by both an encryption key of the destination party to which the message will be passed, as well as by the ephemeral encryption key indicated by the ephemeral encryption key identifier. The message body portion is encrypted with the symmetric key included in the message key portion *[0036]*, *which reads on* receiving an identifier associated with the node and forwarding the wrapped value to another node at an address associated with the identifier comprising a URL.

As per claim 15 *Hanna* teaches party A encrypting the message body using a symmetric key, encrypting that symmetric key and party B decrypting the symmetric key using it later to decrypt the body of the message *[0039-0040] which reads on* encrypting information with the first secret key to form an encrypted information value, communicating the encrypting information value which then is decrypted and use to decrypt the encrypted information value.

As per claim 17 *Hanna* teaches a key identifier associated with said second decryption key *(Fig. 5, object 84)*. Using said key identifier to select said second decryption key from a plurality of decryption keys accessible by said second node is implicit.

Claims 27-29 and 32-34 are substantially equivalent to claims 1-3; therefore claims 27-29 and 32-34 are similarly rejected.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 11-14 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Hanna (U.S. Pub. No.2002/0136410)* in view of Official Notice.

15. As per claim 11 *Hanna* teaches a method as discussed above.

16. *Hanna* does not teach encrypting a doubly wrapped value with a fourth encryption key to form an encrypted doubly wrapped value, wherein said

fourth encryption key has a corresponding fourth decryption key; encrypting said fourth decryption key with said second encryption key, communicating said encrypted fourth decryption key and said doubly wrapped value from said first node to said second node, decrypting said encrypted fourth decryption key to obtain said fourth decryption key using said second decryption key in the event said second decryption key has not expired, and decrypting said encrypted doubly wrapped value using said fourth decryption key to obtain said doubly wrapped value.

Official Notice is taken that it is old and well-known to encrypt data communicated between entities with a symmetric key in order to increase security of data.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use a fourth symmetric encryption key corresponding to the fourth decryption key. One of ordinary skill in the art would have been motivated to perform such a modification in order to increase data security.

Since as discussed above *Hanna* teaches that the decrypting process is iterative *[0042]* it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to encrypt said fourth decryption key with the second encryption key encrypting said fourth decryption key with the second encryption key. One of ordinary skill in the art would have been motivated to perform such a modification in order to allow the next *(ephemeral)* decryption node to be able to decrypt the fourth key in order to decrypt a doubly wrapped value. Encrypting the fourth decryption key would assure security.

Communicating said encrypted fourth decryption key and said doubly wrapped value from said first node to said second node, decrypting said encrypted fourth decryption key to obtain said fourth decryption key using said second decryption key in the event said second decryption key has not expired, and decrypting said encrypted doubly wrapped value using said fourth decryption key to obtain said doubly wrapped value would be implicit.

17. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Hanna (U.S. Pub. No.2002/0136410)*.

Hanna teaches a method as discussed above.

Hanna does not explicitly teach the step of deleting the first secret key subsequent to decrypting the encrypted information value.

However, *Hanna* teaches that an encrypted message may remain in existence well beyond its usefulness which may result in the privacy of the message being compromised and that the encrypted data cannot be recovered following the destruction of the decryption key *[0007-0008]*. Decrypting the encrypted information value would allow the need for the encrypted information value; therefore it would have been obvious to one having ordinary skill in the art to delete the first secret key subsequent to decrypting the encrypted information value.

18. Claims 18-21, 23, 26, 30-31 and 35-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Hanna (U.S. Pub. No.2002/0136410)* in view of *Jenkins et al. (U.S. Patent No. 5812669)* and in further view of Official Notice.

As per claim 18 *Hanna* teaches a three party system depicted in FIG. 9 in which one of the nodes in conjunction with a tamper resistant cryptographic processor unit serves as an ephemerizer and the other two nodes are involved in message communication *[48]*. Node B transmits an ephemeral message to Node C encrypting its message with a first encryption key for which Node C holds the corresponding first decryption key. These first encryption and decryption keys comprise a public/private key pair. Node B then encrypts the message encrypted with the first encryption key with the ephemeral encryption key to form an ephemeral message. The ephemeral message is then forwarded to Node C. The ephemeral message may include an address of the ephemerizer (Node A with cryptographic processor unit) in the form of a uniform resource locator (URL) or any other suitable identification to facilitate the forwarding of information from Node C to Node A for decryption by the ephemerizer *[0053]*. The ephemeral message of information within the message is then passed from Node C to Node A for communication to the tamper resistant cryptographic processor unit. The forwarded message includes an ephemeral key identifier that was obtained with the ephemeral public key *[0054]*.

This reads on receiving at a first node a doubly wrapped value encrypted with a second encryption key to form the doubly wrapped value and on the singly wrapped value encrypted with a second encryption key to form the doubly wrapped value.

Furthermore, *Hanna* teaches the cryptographic processor unit using the ephemeral key pair identifier to identify the applicable expiration time the forwarded message including an ephemeral key identifier that was obtained with the ephemeral public key. The cryptographic processor unit uses the applicable ephemeral decryption key to decrypt the ephemeral message, which is then sent to Node C *[0055-0057]*.

This reads on obtaining at said first node a second decryption key associated with the second encryption key, the second decryption key having a predetermined expiration time, decrypting the doubly wrapped value using the second decryption key to obtain the singly wrapped value in the event the second decryption key has not expired and securely communicating the singly wrapped value to the second node.

Hanna does not explicitly teach receiving at the first node an integrity verification key securely associated with the doubly wrapped value.

Jenkins et al. teach a sender computing a digital signature, which then is sent to the recipient that verifies the signature *(Jenkins et al., col. 2 lines 23-48)*.

The digital signature *reads on* proof that a sender is an authorized decryption agent for said value and on verifying the proof by the receiver using the integrity verification key to ascertain whether the sender is an authorized decryption agent for the value.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to communicate from a second node to the first node proof that the second node is an authorized decryption agent for said value and verifying the proof at first node using the integrity verification key to ascertain whether the second node is an authorized decryption agent for the value as taught by *Jenkins et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to assure data integrity and non-repudiation of origin *(col. 2 lines 45-49, Jenkins et al.).*

As per claim 26 *Hanna* teaches the benefit of minimizing the amount of the message encrypted using the ephemeral keys *[0029]*; therefore it would have been obvious to one having ordinary skill in the art to encrypt the information payload with a secret key and encrypt the secret key with the ephemeral keys as shown in Fig. 2.

19. Claims 30-31 and 35-36 are substantially equivalent to claim 18; therefore claims 30-31 and 35-36are similarly rejected.

20. Claims 22, 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Hanna (U.S. Pub. No.2002/0136410)* in view of *Jenkins et al. (U.S. Patent No. 5812669)* and in further view of Official Notice.

21. As per claim 22 the integrity verification key comprises said first public key associated with the second node is implicit; the digital signature is produced with the second node private key and can be verified only with second node public key.

Hanna in view of *Jenkins et al.* don't teach securely associating a step including the step of encrypting the singly wrapped value and the first public key with said second encryption key

Official Notice is taken that it is old and well-known to encrypt data communicated between entities in order to increase security of data.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to encrypt data communicated between the first and the second node, including the singly wrapped value and the first public key with said second encryption key. One of ordinary skill in the art would have been motivated to perform such a modification in order to increase data security.

As per claim 24 *Hanna* in view of *Jenkins et al.* don't teach securely communicating the singly wrapped value from the first node to the second nod including encrypting the singly wrapped value with a third encryption key to form an encrypted singly wrapped value, wherein the third encryption key has a corresponding third decryption key accessible to the second node and communicating the encrypted singly wrapped value from the first node to the second node.

Similarly to the previously stated Official Notice argument it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to encrypt singly wrapped value from the first node to the second node using second node's public key and for the second node to use it's private key to decrypt the singly wrapped value. One of ordinary skill in the art would have been motivated to perform such a modification in order to increase data security.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Signature

11/23/04

Date

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100